Discrete Mathematics 46 (1983) 49–54
North-Holland

HAMILTONIAN CIRCUITS IN CAYLEY GRAPHS

Dragan MARUŠIČ
Vojke Šmuc 12, 66000 Koper, Yugoslavia

Received 27 July 1982

The following result is proved: If either G is a finite abelian group or a semidirect product of a cyclic group of prime order by a finite abelian group of odd order, then every connected Cayley graph of G is hamiltonian.

1. Introduction

It was conjectured by Lovász in 1969 [2, p. 497] that every connected vertex symmetric graph has a hamiltonian path. Apparently, only four non-trivial connected vertex symmetric graphs without hamiltonian circuits are known [1]. All four possess hamiltonian paths. However, none of these four graphs is a Cayley graph. This inspired many people to conjecture that every connected Cayley graph with more than two vertices has a hamiltonian circuit.

It is fairly easy to see that every connected Cayley graph of an abelian group of order at least 3 has a hamiltonian circuit (Corollary 3.2). However, the main aim of this paper is to prove that the connected Cayley graphs of semidirect products of cyclic groups of prime order by finite abelian groups of odd order are hamiltonian.

2. Preliminaries

All groups considered in this paper are understood to be finite. By a graph we shall always mean a finite, undirected graph without loops or multiple edges.

If Γ is a graph, then $V(\Gamma)$ and $E(\Gamma)$ will denote the set of vertices and the set of edges of Γ, respectively. A graph Γ is said to be *hamiltonian* if it has a hamiltonian circuit, that is, a circuit of length $|V(\Gamma)|$.

Let G be a group. Then id will denote the identity element. If $g \in G$, then $|g|$ will denote the order of g. If M is a subset of G, then M^{-1}, M_0, M^* and $\langle M \rangle$ will denote $\{x^{-1}: x \in M\}$, $M-\{\mathrm{id}\}$, $M_0 \cup M_0^{-1}$ and the subgroup of G generated by M, respectively. If $\langle M \rangle = G$, then M is called a *generating set* of G. If M is a generating set of G and $\langle M-\{x\} \rangle$ is a proper subgroup of G for each $x \in M$, then M is called a *minimal generating set* of G. A *sequence* on G is a sequence all of whose terms are elements of G. By $\square$ we shall denote the *empty* sequence on G, that is, the sequence with no terms. All other sequences on G will be called *non-empty*. Let $S=[s_1, s_2, \ldots, s_r]$ and $T=[t_1, t_2, \ldots, t_q]$ be sequences on G. The *ith partial product* $\pi_i(S)$ of S is $s_1 s_2 \cdots s_i$. Sometimes it will be convenient to use the notation $\pi(S)$ for $\pi_r(S)$. We say that S is *hamiltonian* if $r=|G|$, $\pi(S)=\mathrm{id}$, and the partial products $\pi_i(S)$ $(i=1,2,\ldots,r-1)$ are all distinct non-identity elements of G. If $s_i \in M$, for $i=1,2,\ldots,r$, then S is called an *M-sequence* on G. Let $\mathscr{H}(M, G)$ denote the set of all hamiltonian M^*-sequences on G. The *inverse sequence* S^{-1} of S is the sequence $[s_r^{-1}, s_{r-1}^{-1}, \ldots, s_1^{-1}]$. If $r\geq 2$, then l_S and $\bar{S}$ will denote s_r and $[s_1, s_2, \ldots, s_{r-1}]$, respectively. By $\hat{S}$ we shall denote the sequence $[s_2, s_3, \ldots, s_{r-1}]$ if $r\geq 3$ and the sequence $\square$ if $r=2$. The *product* ST is defined to be the sequence $[s_1, s_2, \ldots, s_r, t_1, t_2, \ldots, t_q]$. By (S, T) we shall denote the sequence $[t_1]\hat{S}^{-1}[t_2]\hat{S}\cdots[t_{q-2}]\hat{S}^{-1}[t_{q-1}]\hat{S}$ if $q\geq 3$ is odd, the sequence $[t_1]\hat{S}^{-1}[t_2]\hat{S}\cdots[t_{q-3}]\hat{S}^{-1}[t_{q-2}]\hat{S}$ if $q\geq 4$ is even and the sequence $\square$ if $q\in\{1,2\}$. For every non-negative integer n we define S^n recursively to be $\square$ if $n=0$ and $S^{n-1}S$ if $n\geq 1$. All these definitions are interpreted in obvious ways when applied to $\square$; for example $S\square=\square S=S$ and $\square^{-1}=\square^n=\square$.

If M is a subset of G, then the *Cayley graph* $\Gamma(G, M)$ is defined to be a graph such that $V(\Gamma(G, M))=G$ and two elements x, y of G are adjacent in $\Gamma(G, M)$ if and only if $xy^{-1}\in M^*$. Clearly, $\Gamma(G, M)$ is a connected vertex symmetric graph, if and only if M is a generating set for G. All Cayley graphs dealt with in this paper will be assumed to have at least three vertices.

The proof of the following lemma is left to the reader.

Lemma 2.1. *The Cayley graph $\Gamma(G, M)$ is hamiltonian if and only if $\mathscr{H}(M, G)\neq\emptyset$.*

The centralizer $C_G(A)$ of a subset A of G consists of all $g\in G$ such that $ga=ag$ holds for all $a\in A$.

If K and H are groups, then a *semidirect product of K by H* is a group G such that K is a normal subgroup of G, H is a subgroup of G, $K\cap H=\mathrm{id}$ and $\langle K\cup H\rangle=G$. It is an easy exercise to see that $G/K\cong H$. (Note that if H also is a normal subgroup of G, then G is a direct product of K and H.)

3. Main results

Lemma 3.1. *Let M be a generating set of an abelian group G and M' be a non-empty subset of M_0. If $S, T\in\mathscr{H}(M', \langle M'\rangle)$ and $l_S=l_T$, then there exists a sequence Q on G such that $\bar{S}Q, \bar{T}Q\in\mathscr{H}(M, G)$.*

Proof. We proceed by induction on the cardinality of $M_0\setminus M'$. The assertion of 3.1 is clearly true if $M_0\setminus M'=\emptyset$. Let $M_0\setminus M'\neq\emptyset$, $g\in M_0\setminus M'$, $H=\langle M\setminus\{g\}\rangle$, and j be the smallest positive integer such that $g^j\in H$. By the induction hypothesis there exists a sequence R on H such that $\bar{S}R, \bar{T}R\in\mathscr{H}(M\setminus\{g\}, H)$. If $W=\bar{S}R$, let Q be the sequence

$$\bar{R}(W,[g]^j)[l_W][g^{-1}]^{j-1}$$

if j is odd and the sequence

$$\bar{R}(W,[g]^j)[g](\bar{W})^{-1}[g^{-1}]^{j-1}$$

if j is even. Then $\bar{S}Q, \bar{T}Q \in \mathscr{H}(M, G)$.

Corollary 3.2. *Every connected Cayley graph of an abelian group of order at least three is hamiltonian.*

Proof. By 2.1 it suffices to show that if M is a generating set of an abelian group G of order at least 3, then $\mathscr{H}(M, G) \neq \emptyset$. If M contains an element x of order $n \geqslant 3$, then let $M' = \{x\}$ and $S = [x]^n$. If M contains no element of order at least 3, then it contains (since G has order at least 3) two distinct elements y, z of order 2. Then let $M' = \{y, z\}$ and $S = ([y][z])^2$. It follows by 3.1 that $\mathscr{H}(M, G) \neq \emptyset$.

Theorem 3.3. *Every connected Cayley graph of a semidirect product of a cyclic group of prime order by an abelian group of odd order is hamiltonian.*

Proof. Let G be a semidirect product of a cyclic group K of prime order p by an abelian group H of odd order, and let L be a generating set of G. If G is abelian, then $\mathscr{H}(G, L)$ is hamiltonian by 3.2. We may therefore assume that G is non-abelian. Thus $|H| \geqslant 3$. Let M be a minimal generating set of G contained in L. Then $M = M_0$. If $p = 2$, then H is a subgroup of index 2 in G. This implies that G is a direct product of two abelian groups K and H and is therefore itself abelian. Hence $p > 2$. Furthermore, since $G/K \cong H$ is abelian, it follows by [4, Exercise 2.47] that

$$[G, G] \subseteq K \tag{1}$$

where $[G, G]$ is the commutator subgroup of G. Let $k \in K_0$. For each $g \in G$ there exists an integer $d(k, g)$ such that $g^{-1}kg = k^{d(k,g)}$ (since K is a cyclic normal subgroup of G). A simple computation shows that

$$d(k, gg') \equiv d(k, g)d(k, g') \pmod p \tag{2}$$

for $g, g' \in G$. Thus if $n = |g|$, then

$$d(k, g)^n \equiv d(k, \mathrm{id}) \equiv 1 \pmod p. \tag{3}$$

Let $e(k, g) = \sum_{i=1}^{n} d(k, g)^i$. Suppose now that $g \notin C_G(K)$. Then $kg \neq gk$ and therefore $k(kg) \neq (kg)k$ and therefore $kg \notin C_G(K)$. Since $g \notin C_G(K)$, it follows that $d(k, g) \not\equiv 1 \pmod p$. Furthermore, $e(k, g)(d(k, g) - 1) = d(k, g)(d(k, g)^n - 1) \equiv 0 \pmod p$ by (3) and so $e(k, g) \equiv 0 \pmod p$. Therefore $(kg)^n = g^n k^{e(k,g)} = \mathrm{id}$ and therefore $|kg| \leqslant |g|$. Similarly, (since $kg \notin C_G(K)$) we deduce that $|k^{-1}(kg)| \leqslant |kg|$.

Hence,

$$\text{if} \quad g \notin C_G(K), \quad \text{then } |kg| = |g| \quad \text{for each } k \in K. \tag{4}$$

Suppose first that M contains an element k of K_0. Let $F = \langle M \setminus \{k\} \rangle$. Since M is a minimal generating set of G, it follows that $K \cap F \neq K$ and therefore $K \cap F = \langle \text{id} \rangle$. Furthermore, $\langle K \cup F \rangle = G$ and therefore G is a semidirect product of K by F. Therefore $F \cong G/K \cong H$ is abelian. Therefore, by 3.2 there exists

$$S = [s_1, s_2, \ldots, s_r] \in \mathcal{H}(M \setminus \{k\}, F).$$

Let

$$T = [k^{-1}]^{p-1}[s_r][k^{-1}]^{p-1}[s_{r-1}] \cdots [k^{-1}]^{p-1}[s_1].$$

Since $K \cap F = \langle \text{id} \rangle$, the partial products $\pi_i(T)$ $(i = 1, 2, \ldots, pr - 1)$ are all distinct non-identity elements of G. Let $z = \sum_{f \in F} d(k, f)$. Since G is non-abelian, there exists $f' \in F \setminus C_G(K)$. By (2)

$$z = \sum_{f \in F} d(k, ff') = \sum_{f \in F} d(k, f) f(k, f') \equiv z d(k, f') \pmod p,$$

$z(d(k, f') - 1) \equiv 0 \pmod p$ Since $f' \notin C_G(K)$, it follows that $d(k, f') \not\equiv 1 \pmod p$ and so $z \equiv 0 \pmod p$. Since $S \in \mathcal{H}(M \setminus \{k\}, F)$, it follows that $\sum_{i=1}^{r} d(k, \pi_i(S)) = z$ and therefore $\pi(T) = ks_r ks_{r-1} \cdots ks_1 = s_r s_{r-1} \cdots s_1 k^z = \pi(S) k^z = \text{id}$. Thus $T \in \mathcal{H}(M, G)$.

Suppose now that $M \cap K = \emptyset$. Since G is non-abelian, there exist $x, y \in M$ such that

$$xy \neq yx. \tag{5}$$

Let ψ be the homormorphism of G onto H such that $g \in K\psi(g)$, for each $g \in G$. Let $a = \psi(x)$, $b = \psi(y)$ Let $|a| = n$. Then n is odd since $|H|$ is odd, and $a \neq \text{id}$ since $M \cap K = \emptyset$. Therefore $n \geq 3$. Similarly, $|b| \geq 3$. Select $c' \in M^* \cap \psi^{-1}(c)$ for each $c \in \psi(M^*)$ in such a way that if $b \notin \{a, a^{-1}\}$, then $a' = x$, $(a^{-1})' = x^{-1}$, $b' = y$, $(b^{-1})' = y^{-1}$. If $R = [r_1, r_2, \ldots, r_t]$ is a $\psi(M^*)$-sequence, then R' will denote the sequence $[r_1', r_2', \ldots, r_t']$.

Suppose first that $b \in \langle a \rangle$. Let i be the least positive integer such that $b = a^i$ Let $A = [a^{-1}]^n$ and B be A if $i \in \{1, n-1\}$ and the sequence $[b][a]^{n-i-1}[b][a^{-1}]^{i-1}$ otherwise. Clearly, $A, B \in \mathcal{H}(\{a, b\}, \langle a \rangle)$ and $l_A = l_B$. By 3.1 there exists a sequence Q on H such that both $S = \bar{A}Q$ and $T = \bar{B}Q$ belong to $\mathcal{H}(\psi(M), H)$. Since $\psi(y) = b = a^i = (\psi(x))^i = \psi(x^i)$, it follows that $y \in Kx^i$. Thus (by (5)) there exists $k \in K_0$ such that $y = kx^i$. If $x \in C_G(K)$, then $yx = kx^{i+1} = xkx^i = xy$, which contradicts (5). Thus $x \notin C_G(K)$ and so by (4), $|x| = |a| = n$. By (3), $d(k, x)^n \equiv 1 \pmod p$ and therefore $d(k, x) \not\equiv -1 \pmod p$ since n is odd.

Let $\tilde{S} = [x^{-1}]^{n-1}Q'$ if $i \in \{1, n-1\}$. Let $\tilde{T}$ be $[y^{-1}][x^{-1}]^{n-2}Q'$ if $i = 1$ and $[y][x^{-1}]^{n-2}Q'$ if $i = n-1$. Suppose that $i \in \{1, n-1\}$. By (5), $x \neq y, y^{-1}$ and therefore $x^{-1}x^{-n+2}\pi(Q')$ is unequal to both $yx^{-n+2}\pi(Q')$ and $y^{-1}x^{-n+2}\pi(Q')$. Therefore $\pi(\tilde{S}) \neq \pi(\tilde{T})$. Therefore $\pi(\tilde{U})$ generates K, where U is one of S or T.

Furthermore, since $U \in \mathscr{H}(\psi(M), H)$, it follows that two different partial products of $\tilde{U}$ do not belong to the same coset of K. Therefore $\tilde{U}^p \in \mathscr{H}(M, G)$. If $i \notin \{1, n-1\}$, then

$$\begin{aligned}\pi(T')\pi(S')^{-1} &= yx^{n-i-1}yx^{-i+2}\pi(Q')\pi(Q')^{-1}x^{n-1}\\ &= yx^{-i-1}yx^{-i+1} = kx^{-1}kx = k^{1+d(k,x)} \neq \mathrm{id}\end{aligned}$$

since we have seen that $d(k, x) \not\equiv -1 \pmod p$. Therefore $\pi(S') \neq \pi(T')$ and thus (as above) either $(S')^p$ or $(T')^p$ belongs to $\mathscr{H}(M, G)$. A similar argument shows that $\mathscr{H}(M, G) \neq \emptyset$ if $a \in \langle b \rangle$.

Suppose now that $b \notin \langle a \rangle$ and $a \notin \langle b \rangle$. If both x and y were in $C_G(K)$, since $x = k_1 a$, $y = k_2 b$ for some $k_1, k_2 \in K$ and $a, b \in H$ and H, K are abelian, it would follow that

$$xy = xk_2b = k_2xb = k_2k_1ab = k_1k_2ba = k_1ya = yk_1a = yx,$$

contradicting (5). We lose no generality in assuming that $x \notin C_G(K)$. Let m be the smallest positive integer such that $b^m \in \langle a \rangle$. Clearly, m is odd and at least 3. Let

$$A = [a]^{n-1}([a]^n, [b]^m)[a][b^{-1}]^{m-1}$$

and

$$B = [a]^{n-1}([a]^n, [b]^{m-2})[b][a^{-1}]^{n-3}[b][a]^{n-1}[b^{-1}][a^{-1}][b^{-1}]^{m-2}.$$

Then $A, B \in \mathscr{H}(\{a, b\}, \langle a, b \rangle)$ and $l_A = l_B$. Hence, by 3.1 there exists a sequence Q on H such that $S = \bar{A}Q$ and $T = \bar{B}Q$ both belong to $\mathscr{H}(\psi(M), H)$. By (1) and (5), $xyx^{-1}y^{-1} \in K_0$ and therefore, since $x \notin C_G(K)$, it follows that $(xyx^{-1}y^{-1})x \neq x(xyx^{-1}y^{-1})$. Therefore, $x^{-2}(xyx^{-1}y^{-1}) \neq x^{-1}(xyx^{-1}y^{-1})x^{-1}$, that is,

$$x^{-1}yx^{-1}y^{-1} \neq yx^{-1}y^{-1}x^{-1}.$$

Since $x \notin C_G(K)$, it follows (by (4)) that $|x| = n$. Thus, (7) implies that $\pi(S') \neq \pi(T')$ so that either $(S')^p$ or $(T')^p$ belongs to $\mathscr{H}(M, G)$.

We have now proved that $\mathscr{H}(M, G) \neq \emptyset$. Consequently $\mathscr{H}(L, G) \neq \emptyset$, and so $\Gamma(G, L)$ is hamiltonian by 2.1.

Since by [4, Theorem 7.13] an extension of an abelian group of order m by any group whose order is relatively prime to m is always a semidirect product, 3.3 yields the following result.

Corollary 3.4. *Every connected Cayley graph of an extension of a cyclic group of prime order p by an abelian group of odd order relatively prime to p is hamiltonian.*

Acknowledgement

The author would like to thank his supervisor Professor C.ST.J.A. Nash-Williams for helpful suggestions during the preparation of this paper.

References

[1] J.A. Bondy, Hamilton cycles in graphs and digraphs, Proc 9th S.E. Conf. Comb., Graph Theory and Computing, (1978) 3–28.

[2] R Guy, H. Hanani, N. Sauer and J. Schonheim, eds., Combinatorial Structures and Their Applications (Gordon and Breach, New York, 1970).

[3] M.B. Nathanson, Partial products in finite groups, Discrete Math. 15 (1976) 210–203.

[4] J.J. Rotman, The Theory of Groups: An Introduction (Allyn and Bacon, Boston, MA, 1965).